RESPONSE

Claims Status

Claims 1-8 were originally filed in this application. In an office action dated December 16, 2004, Claims 1-8 were rejected, and an amendment and response was filed on May 9, 2005 in response thereto. A final office action was mailed on August 5, 2005, maintaining the rejection of claims 1-8. A subsequent amendment and response was filed on December 5, 2005, as part of a request for continued examination in which Applicant amended the specification, cancelled claims 1 and 6-8, amended claims 2-5, and added new claims 9-16. In an office action dated March 6, 2006, claims 2-5 and 9-16 were rejected. A subsequent amendment and response was filed on May 25, 2005, in which Applicant amended claims 4, 5, 9, 11, 13, 15 and 16. A final office action was mailed on July 31, 2006, in which new grounds for rejection were cited. In response, Applicant submitted an amendment and response to address these new rejections.

In an office action dated December 11, 2006, the claims were again rejected under 35 U.S.C. §103(a). Applicant now submits an amendment and response addressing these rejections, in which claims 2, 3, 5, 9, 11 and 16 have been amended. No new matter has been added.

Claim Objections

Claims 3, 5, 9, 11 and 16 have been objected to for certain non-substantive issues. Applicant has amended these claims to address these objections, and respectfully request the withdrawal of these objections.

Claim Rejections

Claims 4-5, 9, 11, 13 and 15-16 have been rejected under 35 U.S.C. 103(a) over U.S. Patent No. 6,735,313 to Bleichenbacher et al. ("Bleichenbacher") in view of U.S. Patent No. 5,029,207 to Gammie ("Gammie").

Claim 2 has been rejected under 35 U.S.C. 103(a) over Bleichenbacher and Gammie and in further view of U.S. Patent No. 5,768,381 to Hawthorne ("Hawthorne").

Independent Claims 9 and 13

Independent claims 9 and 13, as amended, each recite using unique packet tags to encrypt or decrypt secure content at transmission (claim 9) or receipt (claim 13). More specifically, claim 9 recites, in part, "creating different packet keys for each data packet" and "encrypting each data packet using the packet keys" where the packet keys are based on a base key "and unique packet tags assigned to each data packet." Likewise, claim 13 recites, in part, "receiving an encrypted packet stream . . . comprising a plurality of packets" where each packet includes "a unique tag value" and "computing different packet keys for each packet based on the unique tag value." As a result, each packet of a given data stream contains information (i.e., the packet tag) that *uniquely identifies the packet* and is used to create encryption and decryption keys for that packet. See, for example, paragraphs [0029] and [0032] of Applicant's published application. None of the cited references consider the use of packet-specific tags to encrypt data packets.

The Office Action points out that Bleichenbacher encrypts media using "a random base key" and a "program identifier" by "applying one or more hash functions to the master key m depending on the binary value of the program identifier, p." Bleichenbacher, col. 5, lines 50-53. While this approach may result in unique packet keys, these packet keys are not based on unique packet tags, as claimed. In fact, the technique used by Bleichenbacher relies on known values (e.g., bit positions) to generate the keys, and therefore must use different hash functions – an added complexity eliminated by using Applicant's approach. Further, Bleichenbacher uses a "program key K_p, which may be unique to the program" not a packet-specific tag to encrypt a data stream, meaning the IDs are only unique at the program level, and thus *are the same for each packet* for a given program. Bleichenbacher does not, therefore, contemplate the use of "unique packet tags" to generate packet-level encryption and decryption keys as recited in each of the independent claims.

Gammie does not cure the deficiencies of Bleichenbacher. Gammie describes a decoder for descrambling encoded video transmissions using a key that is encrypted using two different serial numbers which are "respectively assigned to a subscriber's decoder and a removable security module." Gammie, col. 8, lines 19-20. Further, the key itself is not based on unique packet identifiers within the content as claimed, instead the decoder uses "a key memory containing *the* key used to scramble [the] program." Gammie, col. 10, lines 11-12 (emphasis added). Clearly, a single key is used to scramble the entire program, and device-specific (not packet-specific) serial numbers are used to encrypt and decrypt the key.

Thus, Applicant respectfully submits that independent claims 9 and 13, as well as those claims that depend therefrom, are patentable over the cited references.

CONCLUSION

Applicant respectfully requests reconsideration of the application and claims in light of this Response, and respectfully submits that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Joel Elehrer

Joel E. Lehrer
Attorney for Applicant
Goodwin Procter LLP
Exchange Place
Boston, Massachusetts 02109
Customer No. 051414

Date: May 11, 2007
Reg. No. 56,401

Tel. No.: (617) 570-1057
Fax No.: (617) 523-1231